Social Engineering

May 2004

Topics

- What is Social Engineering?
- Social Engineering Methods & Techniques
- Goals of Social Engineering
- Impact
- How to Identify Social Engineering
- Preventative Measures and Solutions
- Examples

Definition

Social Engineering is a term used to describe unauthorized users, business competitors and hackers attempting to gather confidential and/or secret information by relying on the weaknesses of people rather than hardware or software; the aim is to trick people into revealing passwords or other information that compromises a target system's security.

Social Engineering Methods

- **Depends on the hackers skill and the type of information they are seeking.**

- **Will perform some research, known as "footprinting" of the target before undergoing further activities. "Footprinting is trying to determine the security posture of an entity and is one of the most important steps." The key to a successful campaign lies more in the preparation than the actual execution.**

- **Social engineering can be non-technical or technical in nature.**

All involve schemes, trickery and deception

Non Technical Methods

- **Utilizing non-technical techniques, the hacker will rely on interpersonal relationships to obtain information.**
- **Examples include:**
  - Shoulder Surfing
  - Social Engineering over the Telephone
  - Dumpster Diving

Non Technical Methods

- **Social Engineering via Shoulder Surfing**

Shoulder surfing is when hackers watch someone type their password and are able to figure out what the user has typed so they can later enter the system with the user's id and password.

As security controls are getting tighter, hackers may find it easier to shoulder surf because users are typing a longer more secure password and are much slower at typing.

The hacker does not have to be behind the user they could be using binoculars or a type of video equipment to capture what the user is typing.

Non Technical Methods

- **Social Engineering via Telephone**
  - Most common technique (can occur at home or at work).
  - An attacker may try to persuade the user over the phone by impersonation, persuasion, friendliness and ingratiation.
  - **Example**: A hacker will call up a help desk and request to speak to a person of high authority (supervisor or LAN Manager) and persuade them that they are a representative from the company that manages their telecommunications equipment or someone of authority or relevance. They will pretend to be calling about a possible problem with the connection and make attempts at obtaining the password to the main system. Through research, they may already have much information gathered on the company before making the attempts to gain access. In most cases, they are successful at getting the information or something close to the information they need to get the access they are seeking to do the damage to.

Non Technical Methods

Social Engineering via Dumpster Diving

- Also known as “trashing”
- Person searching through dumpsters for information
- Gather information such as employee names, contact numbers, email addresses or any information that could be useful to them
- Sources include: Department phone books, org charts, Department policy manuals, memos, event calendars, vacation schedules, system manuals, login names and passwords, printouts of sensitive information, source code printouts, disks and tapes, credit card statements, bills, statements, and outdated hardware or software

Dumpster Diving Cont.

- All the information gathered gets the hacker's one step closer to getting what they want. If they are trying to impersonate a manager, they could get information about him/her off the organizational chart. The memos could give information about a person going on vacation and the hacker's an use this to impersonate the person gone. Old system manuals give instructions on how to enter the system or possible vulnerabilities of the system.

- Reports can open the door for the hacker with a user's id and password. Calendars can let the hacker know when a person is at a meeting or out of the office. They then are known to go into an office and take over a person's computer. Disks full of information can be the "keys to the kingdom", where little pieces of information can be gathered that could allow them into the building or system. Several companies have provided recycling bins as well as locked bins that are to be disposed of in an effort to fight against dumpster diving. This has helped considerably but there are those users who think it's a waste e of time and just toss the paper in the garbage.

Technical Methods

- **Utilizing technical methods, the hacker will rely on technology to trick an individual into supplying further information.**

- **Examples:**
  - Social Engineering via Internet or Online
  - Social Engineering via Instant Messaging

Technical Methods

- **Social Engineering via Internet or Online**
  - Filling out forms online that request information about the number of systems we have in the network, types of operating systems, software and applications being used.
  - Receive offers for free gifts via email or banners on WebPages that will make requests for personal information include social security numbers, credit card info, employer information, job title, etc.
  - Websites that request that you register a username and password in order to obtain the information you need or in order to get something being offered.
  - Via Instant Messaging services. Users are tricked into downloading software, or executing malicious code (sent in messages soliciting pornography, anti-virus software, applications that will improve system performance or provide enhanced features) that will give an intruder access to the system to use as a platform in launching denial of service attacks.

Technical Techniques

Social Engineering via Instant Messaging

- **Example** of a Message Received via IM: You are infected with a virus that will allow hackers access to your machine at IP address 129.221.092.109 and they will have access to your files, etc. With our software, you can prevent this from happening, visit our site at www.badbadhackerpeople.com to download this software instantly and clean your infected machine.

Techniques for Social Engineering

If someone is going to use a non technical approach, the success of their actions will depend on what technique and approach they use.

Some techniques are easier than others.

Examples:

- **Direct Approach**
- **Passive Approach**
- **Pose as an Important User**
- **Pose as a helpless or new user**
- **Reverse Engineering Approach**

Common Techniques

If done right, some users will provide the impersonator with the information they seek.

- **Direct Approach/Persuasion**
  - Easiest approach
  - More straightforward method
  - Very little information is being requested so as to keep suspicions low
  - In person, the hacker may use a fake ID and they will dress the part they intend to portray
  - A hacker may ask a user directly to perform a task for instance, posing as someone from the help desk and requests a username and password in order to assist with a network problem
  - Most people will be less likely to be persuaded to provide their password to anyone requesting it via telephone or any other means.

Common Techniques

- **Pose as an Important User Approach**
  - The hacker may contact the user posing as a top official (with a deadline) in the organization and intimidates the user into providing the information they seek.
  - User can be pressured into providing information about:
    - Configuring the network for remote access
    - Type of applications being used for remote access
    - Dial up numbers
    - Username and password for entry to the system platform

Common Techniques

- **Posing as the helpless/new user approach**
  - More common method used
  - Pretending to be a new user to the system needing access to the network resources
  - Easy for a hacker to impersonate this type of user and succeed
  - Can pretend to be clueless about the system and still gain information that will give him access to it

A simple tactic that a hacker may use to gain access to your network.

Common Techniques

- **Reverse Engineering Approach-**

- **Hacker poses as someone in a position of authority, like help desk, and encourages employees to ask him for information.**

- **Harder to carry out because hacker must be knowledgeable of the system and may have previously had access to that system via normal means.**

- **Legitimate system users ask a hacker questions to gain information.**

May offer a greater chance for the hacker to gain information about the company through the employees

Stages of Reverse Social Engineering

Three parts of RSE are:

- Sabotage
- Advertising/Marketing
- Assisting/Support

1. **The hacker will sabotage a network to cause a problem to arise.**

2. **Then he advertises that he is the POC to fix the problem. This can be done by leaving business cards around the office, or replacing contact numbers on the original error message with numbers that lead directly to him for further support.**

3. **He will assist with the problem and ensures his identity remains undiscovered as he seeks to gain the information he needs.**

User never realize person was a hacker because their network problems disappear and everyone is happy.

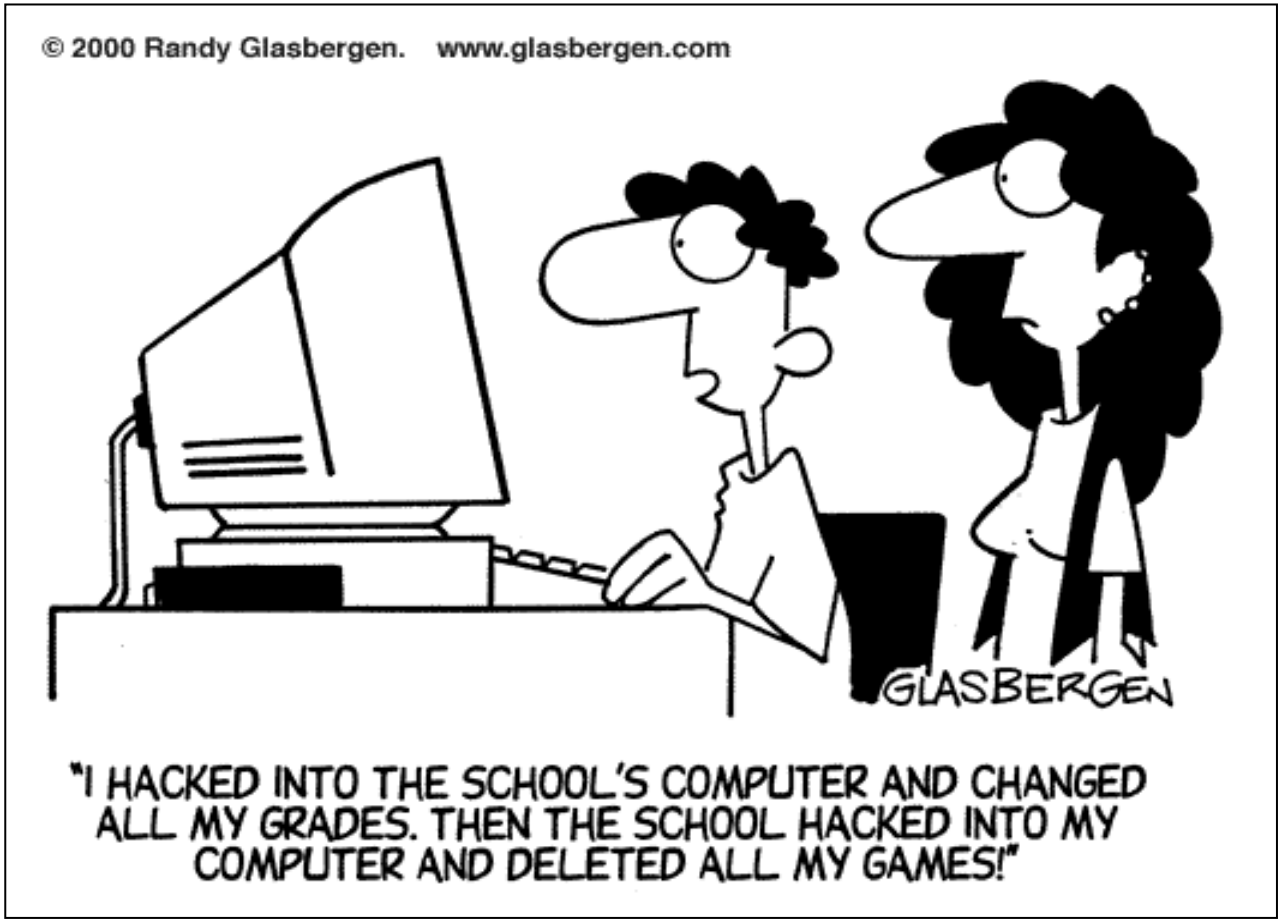
Common Techniques

- **The Passive Approach**
  - Does not involve direct contact with the victim
  - Can be tied with another method such as impersonation
  - Examples:
    - Shoulder surfing
    - Email solicitation
    - Dumpster diving

Goals of the Social Engineer

- Financial Gain
- Identity Theft
- Perpetrate Industrial Espionage
- Gain Sensitive or Critical Information
- Entertainment (fun)
- Network Intrusion

Impact



A hacker or intruder can gain access to a system through the unauthorized use of accounts that have been compromised.

Identifying Social Engineering

- Too friendly
- In too much of a rush
- Being too polite
- Dropping names
- Oversight
- Overconfidence
- Requesting entry into an area alleging loss of key or badge
- If via phone, background noise or interference such as “street noise” are not ‘in sync’ with the situation
- Too many inappropriate questions

Preventative measures (Solutions)

Preventative measures (Solutions)

Do not let anyone at anytime stand behind them while typing their id and password.

Shred any sensitive documents when done with them.

Question people that call you asking for personal information. If something sounds fishy, trust your instincts and end the conversation.

For More Information

- **These documents are another good resource: http://www.giac.org/practical/GSEC/Diana_Carmany_GSEC.pdf.**

- **http://www.giac.org/practical/Chan_Lieu_GSEC.doc.**